CLAIMS

1. A secret key generating method for generating a secret key of an entity in each of a plurality of key generating agencies, comprising the steps of:

obtaining each divided identification information by dividing identification information of the entity into a plurality of blocks;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information; and

generating a secret key of the entity by synthesizing the extracted components with a random number particular to the entity.

2. The secret key generating method according to claim 1, wherein the random number which is to be synthesized in a first key generating agency is generated based on a hash function generated in the first key generating agency and a hash function generated in one or plural key generating agency except the first key generating agency.

3. The secret key generating method according to claim 2, wherein J key generating agencies exist, the j-th (j = 1, 2, ..., J) key generating agency sends the hash function, which the agency itself has generated, to the (j + 1)-th, (first in the case of j = J), key generating agency and, in the (j + 1)-th, (first in the case of j = J), key generating agency the random number which is to be synthesized in the agency itself is generated based on the hash

function which the agency itself has generated and on the hash function of the j-th key generating agency which has been sent.

4. A secret key generating method for generating a secret key of an entity in each of a plurality of key generating agencies, comprising the steps of:

obtaining each divided identification information by dividing identification information of the entity into a plurality of blocks;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information; and

generating a secret key of the entity by masking the extracted components with the mask pattern.

5. A secret key generating method for generating a secret key of an entity in each of a plurality of key generating agencies, comprising the steps of:

obtaining each divided identification information by dividing identification information of the entity into a plurality of blocks;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information;

and

generating a secret key of the entity by masking the extracted components with the mask pattern and by synthesizing the mask result with a random number particular to the entity.

6. The secret key generating method according to claim 5, wherein the random number which is to be synthesized in a first key generating agency is generated based on a hash function generated in the first key generating agency and a hash function generated in a second key generating agency.

7. The secret key generating method according to claim 6, wherein J key generating agencies exist, the j-th (j = 1, 2, ..., J) key generating agency sends the hash function, which the agency itself has generated, to the (j + 1)-th, (first in the case of j = J), key generating agency and, in the (j + 1)-th, (first in the case of j = J), key generating agency the random number which is to be synthesized in the agency itself is generated based on the hash function which the agency itself has generated and on the hash function of the j-th key generating agency which has been sent.

8. An encryption method for encrypting a plaintext to be transmitted from one entity to other entity, comprising the steps of:

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information which has been obtained by dividing identification information of the one entity into a plurality of blocks;

generating a secret key of the one entity by synthesizing the extracted components with a random number particular to the one entity;

generating a common key by using a component corresponding to the other entity which is included in the secret key of the one entity; and

encrypting the plaintext into a ciphertext by using the generated common key.

9. An encryption method for encrypting a plaintext to be transmitted from one entity to other entity, comprising the steps of:

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information which has been obtained by dividing identification information of the one entity into a plurality of blocks;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information;

generating a secret key of the one entity by masking the extracted components with the mask pattern;

generating a common key by using a component corresponding to the other entity which is included in the secret key of the one entity; and

encrypting the plaintext into a ciphertext by using the generated common key.

10. An encryption method for encrypting a plaintext to be

transmitted from one entity to other entity, comprising the steps of:

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information which has been obtained by dividing identification information of the one entity into a plurality of blocks;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information;

generating a secret key of the one entity by masking the extracted components with the mask pattern and by synthesizing the mask result with a random number particular to the one entity;

generating a common key by using a component corresponding to the other entity which is included in the secret key of the one entity; and

encrypting the plaintext into a ciphertext by using the generated common key.

11. A common key generating method for generating a common key which is used for an encryption process from a plaintext to a ciphertext and a decryption process from a ciphertext to a plaintext in a cryptographic communication between entities, comprising the steps of:

extracting components which are included in each secret key of one entity and correspond to another entity of the communication partner, each secret key being generated by using each divided identification information obtained by dividing identification

information of the one entity into a plurality of blocks; and

generating a common key by synthesizing the extracted components through XOR.

12. A common key generating method for generating a common key which is used for an encryption process from a plaintext to a ciphertext and a decryption process from a ciphertext to a plaintext in a cryptographic communication between entities, comprising the steps of:

extracting a part of components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information obtained by dividing identification information of one entity into a plurality of blocks;

generating a secret key of the one entity by synthesizing the extracted components with a random number particular to the one entity;

extracting components which are included in the secret key of the one entity and correspond to another entity of the communication partner; and

generating a common key by synthesizing the extracted components through XOR.

13. A common key generating method for generating a common key which is used for an encryption process from a plaintext to a ciphertext and a decryption process from a ciphertext to a plaintext in a cryptographic communication between entities, comprising the steps of:

extracting a part of components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information obtained by dividing identification information of one entity into a plurality of blocks;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information;

generating a secret key of the one entity by masking the extracted components with the mask pattern;

extracting components which are included in the secret key of the one entity and correspond to another entity of the communication partner; and

generating a common key by synthesizing the extracted components through XOR.

14. A common key generating method for generating a common key which is used for an encryption process from a plaintext to a ciphertext and a decryption process from a ciphertext to a plaintext in a cryptographic communication between entities, comprising the steps of:

extracting a part of components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information obtained by dividing identification information of one entity into a plurality of blocks;

generating a mask pattern particular to each key generating agency in accordance with each divided identification information;

generating a secret key of the one entity by masking the

extracted components with the mask pattern and by synthesizing the mask result with a random number particular to the one entity;

extracting components which are included in the secret key of the one entity and correspond to another entity of the communication partner; and

generating a common key by synthesizing the extracted components through XOR.

15. A cryptographic communication method for carrying out an information communication using a ciphertext between a first and second entities, comprising the steps of:

obtaining each divided identification information by dividing identification information of the first and second entities into a plurality of blocks, respectively;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information, respectively;

generating a secret key for the first and second entities, respectively, by synthesizing the extracted components with a random number particular to the first and second entities, respectively;

generating a first common key by using components which are included in the secret key of the first entity and correspond to the second entity;

encrypting a plaintext into a ciphertext by using the generated first common key;

generating a second common key which is identical to the first common key by using components which are included in the secret key of the second entity and correspond to the first entity; and

decrypting the ciphertext into a plaintext by using the generated second common key.

16. The cryptographic communication method according to claim 15, wherein components which are included in respective secret keys of the first and second entities and which correspond to the second and first entities are extracted, respectively, so that the extracted components are synthesized through XOR so as to generate, respectively, the first and second common keys.

17. A cryptographic communication method for carrying out an information communication using a ciphertext between a first and second entities, comprising the steps of:

obtaining each divided identification information by dividing identification information of the first and second entities into a plurality of blocks, respectively;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information, respectively;

generating a mask pattern particular to each key generating agency, respectively, in accordance with each divided identification information, respectively;

generating a secret key for the first and second entities,

respectively, by masking the extracted components with the mask pattern, respectively;

generating a first common key by using components which are included in the secret key of the first entity and correspond to the second entity;

encrypting a plaintext into a ciphertext by using the generated first common key;

generating a second common key which is identical to the first common key by using components which are included in the secret key of the second entity and correspond to the first entity; and

decrypting the ciphertext into a plaintext by using the generated second common key.

18. The cryptographic communication method according to claim 17, wherein components which are included in respective secret keys of the first and second entities and which correspond to the second and first entities are extracted, respectively, so that the extracted components are synthesized through XOR so as to generate, respectively, the first and second common keys.

19. A cryptographic communication method for carrying out an information communication using a ciphertext between a first and second entities, comprising the steps of:

obtaining each divided identification information by dividing identification information of the first and second entities into a plurality of blocks, respectively;

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information, respectively;

generating a mask pattern particular to each key generating agency, respectively, in accordance with each divided identification information, respectively;

generating a secret key for the first and second entities, respectively, by masking the extracted components with the mask pattern, respectively, and by synthesizing the mask result with a random number particular to the first and second entities, respectively;

generating a first common key by using components which are included in the secret key of the first entity and correspond to the second entity;

encrypting a plaintext into a ciphertext by using the generated first common key;

generating a second common key which is identical to the first common key by using components which are included in the secret key of the second entity and correspond to the first entity; and

decrypting the ciphertext into a plaintext by using the generated second common key.

20. The cryptographic communication method according to claim 19, wherein components which are included in respective secret keys of the first and second entities and which correspond to

the second and first entities are extracted, respectively, so that the extracted components are synthesized through XOR so as to generate, respectively, the first and second common keys.

21. A cryptographic communication system for mutually carrying out, among a plurality of entities, an encryption process for encrypting into a ciphertext a plaintext which is information to be transmitted and a decryption process for decrypting the transmitted ciphertext into a plaintext, comprising:

a plurality of key generating agencies, each of which extracts a part of the components of a symmetric matrix of its own secret in accordance with each divided identification information obtained by dividing identification information of each entity into a plurality of blocks and generates a secret key of each entity by synthesizing the extracted components with a random number particular to each entity; and

a plurality of entities, each of which generates a common key which is used for the encryption process and decryption process by using components corresponding to the entity of the communication object which are included in its own secret keys sent from the key generating agencies.

22. A cryptographic communication system for mutually carrying out, among a plurality of entities, an encryption process for encrypting into a ciphertext a plaintext which is information to transmitted and a decryption process for decrypting the transmitted ciphertext into a plaintext, comprising:

a plurality of key generating agencies, each of which extracts a part of the components of a symmetric matrix of its own secret in accordance with each divided identification information obtained by dividing identification information of each entity into a plurality of blocks, generates a mask pattern particular to its own in accordance with each divided identification information and generates a secret key of each entity by masking the extracted components with the mask pattern; and

a plurality of entities, each of which generates a common key which is used for the encryption process and decryption process by using components corresponding to the entity of the communication object which are included in its own secret keys sent from the key generating agencies.

23. A cryptographic communication system for mutually carrying out, among a plurality of entities, an encryption process for encrypting into a ciphertext a plaintext which is information to be transmitted and a decryption process for decrypting the transmitted ciphertext into a plaintext, comprising:

a plurality of key generating agencies, each of which extracts a part of the components of a symmetric matrix of its own secret in accordance with each divided identification information obtained by dividing identification information of each entity into a plurality of blocks, generates a mask pattern particular to its own in accordance with each divided identification information and generates a secret key of each entity by masking the extracted components with the

mask pattern and by synthesizing the mask result with a random number particular to each entity; and

a plurality of entities, each of which generates a common key which is used for the encryption process and decryption process by using components corresponding to the entity of the communication object which are included in its own secret keys sent from the key generating agencies.

24. A computer memory product having computer readable program code means for causing a computer to generate a secret key of an entity, by using each divided identification information obtained by dividing identification information of the entity into a plurality of blocks, and by using a secret symmetric matrix, said computer readable program code means comprising:

program code means for causing the computer to extract a part of the components of the symmetric matrix in accordance with each divided identification information; and

program code means for causing the computer to generate a secret key of the entity by synthesizing the extracted components with a random number particular to the entity.

25. A computer memory product having computer readable program code means for causing a computer to generate a secret key of an entity, by using each divided identification information obtained by dividing identification information of the entity into a plurality of blocks, and by using a secret symmetric matrix, said computer readable program code means comprising:

program code means for causing the computer to extract a part of the components of the symmetric matrix in accordance with each divided identification information;

program code means for causing the computer to generate a mask pattern in accordance with each divided identification information; and

program code means for causing the computer to generate a secret key of the entity by masking the extracted components with the mask pattern.

26. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a secret key of an entity, by using each divided identification information obtained by dividing identification information of the entity into a plurality of blocks, and by using a secret symmetric matrix, comprising:

a code segment for causing the computer to extract a part of the components of the symmetric matrix in accordance with each divided identification information; and

a code segment for causing the computer to generate a secret key of the entity by synthesizing the extracted components with a random number particular to the entity.

27. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a secret key of an entity, by using each divided identification information obtained by dividing

identification information of the entity into a plurality of blocks, and by using a secret symmetric matrix, comprising:

a code segment for causing the computer to extract a part of the components of the symmetric matrix in accordance with each divided identification information;

a code segment for causing the computer to generate a mask pattern in accordance with each divided identification information; and

a code segment for causing the computer to generate a secret key of the entity by masking the extracted components with the mask pattern.